PERSONAL COMPUTER SECURITY

The following is provided to assist the IITSM in the review and/or development of local personal computer security policies and procedures. These items are appropriate whether the unit is a standalone or part of a network.

A. All terminals or PCs should be located in an area where they can be secured and/or effectively monitored by authorized users.

B. System managers and IITSMs should know the location of each PC and the individuals with authorized access.

C. System managers/IITSMs should monitor the use of PCs connected to networks to ensure they are not used to archive or otherwise compromise sensitive data or to modify or load unauthorized programs.

D. For all "sensitive" applications, locate monitors facing away from open doors, windows, or other traffic areas where possible. Where monitors cannot be so positioned, monitor privacy screens should be utilized.

E. In contingency situations, rapid and accurate identification of backup files is vital to proper and timely recovery. All backup media should be labeled according to its sensitivity and/or criticality.

F. Only authorized copies of commercial software should be used on the system. Copying of such software for personal use is prohibited.

G. All hardware, software, documentation, and files must be accounted for upon transfer or termination of employment of any system user.

H. Removal of Government owned PCs, peripheral devices, supplies, or recording media from the workspace is prohibited without the express permission of the system owner/system manager. This includes removal by maintenance personnel and system users.

I. Employees should receive approval from their supervisor before bringing a personally owned PC onto Service premises.

J. Records created, used, stored, etc. on personally owned devices for official Government work are the property of the Government and, as such, are subject to records management procedures and directives. Government data stored on personally owned PCs should not be encrypted.

K. Personally owned computers should not be connected to any Government-owned networks, telecommunications equipment, or storage devices without express permission of the network manager or other relevant system manager.

L. Government information/software must not be used for private profit or purpose.

M. Individuals assume full responsibility for exercising due diligence to protect their equipment from theft. Failure to take appropriate safeguards could result in disciplinary action or having to incur replacement costs.

N. The Service is generally not liable for consequential damage occurring to privately owned equipment**.**

O. Portable computers, laptops, and PDAs are subject to additional risks; therefore, some further cautions are warranted:

(1) Portable computing devices are a high-value item and easily stolen. When traveling with these devices, do not leave them unattended. Due to the greatly enhanced risk of theft, processing of sensitive information on these devices should not be allowed without express permission of the system manager.

(2) While using public transport, do not check portable devices as luggage or otherwise surrender control. It must be kept with you at all times.

(3) For devices containing sensitive information, have them handchecked rather than electronically examined by airport X-ray machines.

P. All computers/laptops should be configured with locked screen savers, requiring a password to gain access.

Q. All computers/laptops should be configured to display the official Government warning message upon boot up.

R. All computers/laptops must have anti-virus software installed and adhere to a defined signature file update schedule.